WRITE ONCE SYSTEM AND METHOD FOR FACILITATING
DIGITAL ENCRYPTED TRANSMISSIONS

The present invention relates to a system and process for facilitating unique code encryption between a computer and an associated peripheral device. In particular, it

5 relates to facilitating HDCP encryption or the like on a digital video interface card which digitally communicates with a digital display or monitor.

BACKGROUND

Digital display devices and other digital peripheral devices are well known in the art. Digital display devices can be designed with video signal inputs to accept either a

10 direct digital signal and/or an analog signal which is converted to digital by the display device. Additionally, some analog display devices accept a digital video signal output.

One concern in the industry is the unauthorized of copying of copyrighted content which may be contained in a video signal. If a video signal is intercepted between transmission from a computer system to a peripheral device, such as a display, it can be

15 used to make virtually identical copies of the video content without any degradation or loss of quality.

Some systems avoid this concern by having an analog output from the computer and an analog input to the digital display device so that only an analog signal may be intercepted. Although copies of the video content can be made based upon the analog

20 signal, there is inherently some degradation and quality loss associated with such an analog signal which compounds when repeated copies are made using analog transmissions. However, where an analog signal is transmitted from the computer to the peripheral digital device, the signal received by the digital device is likely to be of a lower quality than if a digital signal were transmitted between the computer and the

25 peripheral device.

In order to facilitate the transmission of digital signals from a computer to a digital peripheral device while inhibiting unauthorized content copying, encryption schemes and

protocols have been developed to encrypt the digital signal before transmission from the computer and then to decrypt the signal in the digital peripheral device. One proposed protocol is High bandwidth Digital Content Protection (HDCP) specification which requires a graphics controller to store a large set of encryption keys that are unique to the

5   interface devices used to output an encrypted digital signal. Under HDCP, each interface device must be allocated its own unique encryption key data. Thus, each interface device or computer system must be individualized. This poses a manufacturing problem since it is more efficient to manufacture on a mass scale computer systems and/or interface cards which are identical.

10   It would be desirable to provide a computer system and/or interface device which can be easily mass produced, but which also can support encryption systems such as HDCP.

SUMMARY

A digital interface device is provided for facilitating key encryption of a digital

15   signal which is communicated from a computer system to an associated peripheral device, such as a digital display device. The peripheral device decrypts the communicated digital signal during use.

The digital interface device may be built into the computer system or provided as a separate interface card. In either case, the resulting system has a digital output port,

20   digital output formatting circuitry associated with the port and an electrically programmable non-volatile memory such as a flash RAM for storing a basic input/output system (BIOS) for, inter alia, controlling digital output formatting. The interface device is configured such that the non-volatile RAM has a specific addressable write-protectable area allocated for storing an encryption key flag at a flag address along with encryption

25   key data. The write-protectable area being rendered read-only when a predetermined flag value is stored at the flag address. Thus, encryption key data may be stored in the specific write-protectable area of the non-volatile RAM in connection with storing the predetermined flag at that flag address such that encryption data cannot be altered when

the non-volatile RAM is subsequently written to, such as when a BIOS stored in the non-volatile RAM is updated or when an attempt is made to tamper with the encryption keys.

Preferably, the digital interface device is configured to receive either a first predetermined flag value in association with key encryption data which first flag value

5   indicates encryption enablement or a second predetermined flag value which second flag value indicates encryption disablement, in which case the digital interface device is permanently disabled from using the key encryption. If neither of the predetermined flags are contained at the flag address, the write-protectable area of the non-volatile RAM is writable to receive either the first flag value with encryption data or the disabling

10   second flag value.

Preferably, the digital peripheral device is a digital display and the digital output port is configured to output a digital video signal. Also, it is preferred to configure the digital interface device as a digital video interface card, but the interface can be directly incorporated into a computer system's motherboard or other configuration which does not

15   require a separate interface card.

The specific area for storing the encryption key flag and data is preferably at least 1k bytes and is preferably located as an address range higher than an address range reserved for a BIOS in the non-volatile RAM.

As a result of the invention, identical interface cards or systems can be mass-

20   produced and thereafter be uniquely enabled or disabled from using a digital encryption system such as HDCP in an efficient cost-effective manner.

BRIEF DESCRIPTION OF THE DRAWINGS

The above, as well as other objects of the present invention will become apparent when reading the accompanying description and drawings in which:

25   Figure 1 is a schematic diagram of a computer and an associated digital display device which uses the digital interface of the present invention.

Figure 2 is a schematic diagram of the digital interface in a preferred add-in card embodiment of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

With reference to Figure 1, a computer system is illustrated having a computer 10 coupled with an associated digital peripheral device, such as digital display device 12. The computer 10 includes a digital video output port 14 which is coupled to a digital

5   signal input port 16 of the digital display device 12 via conventional means such as a cable 18. The digital video signal output 14 is controlled by a digital interface device 20 such as an add-in card as illustrated in Figure 2. The digital interface device may also include an analog port 22 so that the computer may output video signals either in digital or analog.

10   The digital interface device or card 20, includes graphic control circuitry 24 typically embodied in a chip known as a graphics controller. In the add-in card embodiment of the interface device 20, the graphics controlling circuitry 24 typically receives and communicates with the rest of the computer 10 via an edge card connector 28 which is typically received in an appropriate slot on a motherboard of the computer

15   10.

The graphics controller circuitry 24 is controlled by a basic input/output system program (BIOS) which is stored in a non-volatile RAM 26 of the interface device 20. The non-volatile RAM 26 is a conventional semi-conductor chip device which retains its memory when powered off. During normal video display operations, the non-volatile

20   RAM acts as a read-only memory (ROM) providing the graphic control circuitry 24 with programming instructions such as, for example, the formatting of the graphic output signals. From time to time, it is desirable to upgrade the BIOS which is accomplished by writing the updated BIOS into the non-volatile RAM 26. This update operation can be controlled by the graphic control circuitry 24.

25   In order to inhibit the unauthorized copying of the digital signal passed through the connecting cable 18, that digital signal may be encrypted. Accordingly, the interface device is designed so that it may optionally be configured to use a proprietary encryption scheme such as HDCP. Under HDCP, the digital interface device must contain unique encryption key data which is not subject to tampering. However, it is often also desirable

to use essentially the same digital interface device in systems which do not use the proprietary encryption system such as HDCP. Accordingly, in order to use the same physical hardware components to construct digital interface devices which can be permanently configured to allow or disallow use of a proprietary encryption scheme such

5   as HDCP, the non-volatile RAM 26 of the digital interface device 20 of the present invention contains a specified write-protectable area 30 of preferably at least 512 bytes which operates as a write-once memory within the non-volatile RAM 26. Accordingly, the control circuitry 24 which controls the writing to the non-volatile RAM 26 is configured to check a specific flag address within the allocated write-once address area

10   30 of the non-volatile RAM 26. Preferably, a flag address check by the controller is conducted automatically on power up of the system and any reinitialization of the graphics controller. If the flag address contains a predetermined value, the specified address area within the non-volatile RAM 26 is write-protected and the controller 24 can only write information into other areas of the non-volatile RAM 26. In lieu of a single

15   flag address, multiple addresses may be provided which are checked for a certain state or combination of states for write protection enablement.

Preferably, the specified area 30 for the encryption information is at the highest address range of the non-volatile RAM 26. For example, if a 64k byte non-volatile RAM is provided having addresses 0x0000 to 0xFFFF, a 1k byte area having addresses from

20   0xFC00 to 0xFFFF (63k to 64k-1) is designated as the specific write-protectable area 30 within the non-volatile RAM for encryption information. Preferably, the encryption key flag address is at the first byte of the specified area, i.e. preferably at 0xFC00 (63k).

The flag itself may have more than one predetermined value to render the entire specified area 30 as write-protected. For example, the interface device can be configured

25   to recognized the ASCII character "H" as a write-protect flag which also indicates enablement of HDCP encryption and the storage of valid HDCP keys within the write-protected block. A value corresponding to ASCII "h" can be used to indicate write-protection, but that the HDCP encryption is disabled. If neither ASCII "H" or "h" is stored at the flag address, the allocated area would not be write-protected in such an

example. Preferably, however, only a single unique flag value is used for each different state, i.e. only "H" for the write protect HDCP encryption enabled state and "h" for write protect HDCP encryption disabled state.

5   Alternatively, the predetermined value may be inferentially set by specifying that the area 30 is write-protected if it contains any value other than, for example, an ASCII "W", thus, indicating the area 30 is writable. Preferably, the "W" value, if used, is initially stored at the flag address when the specified area 30 is allocated.

If the interface devices were shipped without a predetermined flag stored at the flag address to write-protect the specified area 30, the interface device could be subject to
10   third party tampering. Accordingly, one of the final production step is preferably to either store encryption keys within the designated area 30 and set the flag address to "H" or set the flag address to "h" to disable HDCP encryption functions. Since royalties may be payable for creating devices which utilize encryption schemes such as HDCP, no royalties would be due with respect to interface devices where the encryption is
15   permanently disabled.

By allocating the highest addresses 0xFC00 to 0xFFFF (63k to 64k-1) to the specified write-protectable area 30, the remainder of the non-volatile RAM at addresses 0x0000 to 0xFBFF (0k to 63k-1) is free to be used for the existing BIOS or any updated BIOS. Typical BIOS images range between 40 to 48k bytes. Accordingly, even if BIOS
20   updates become larger in size, there is sufficient room within a 64k byte flash RAM to be accommodated since only the uppermost kilobyte of the flash RAM is used. If a 128K flash RAM is utilized, the write-protectable area 30 is preferably located at address range 0x1FC00 to 0x1FFFF (127k to 128k-1) with the flag address at 0x1FC00 (127k).

Before the flag is set, the specified write-protectable area 30 can be written into in
25   a manner suitable for storing the encryption information. Preferably, the first four bytes of the area receive values corresponding to ASCII characters "H", "D", "C", "P", when the area is written to with encryption key data of the type usable by the HDCP encoding system. Preferably, the first thirteen bytes of the area 30 are written with values

corresponding to ASCII characters "h", "d", "c", "p", " ", "d", "i", "s", "a", "b", "l", "e", "d", when written to permanently disable HDCP encryption.

<div align="center">*   *   *</div>